Security Policies

Stephen H. Hess, University of Utah

2005 Annual Security Conference
Digital Citizenship - Utah at Risk

March 7 - 8, 2005

Sponsored by

Utah!
Where ideas connect™

UEN
UTAH EDUCATION NETWORK
WWW.UEN.ORG

UTAH STATE OFFICE OF EDUCATION

ITS Customer Driven Technology
Information Technology Services

Policy: X-X
Date: December 15, 2003

Subject: **University Information Technology Resource Security Policy**

I. PURPOSE

University Information Technology Resources are at risk from potential threats such as human error, accident, system failures, natural disasters, and criminal or malicious action.

The purpose of this policy is to secure the private sensitive information of faculty, staff, patients, students, and others affiliated with the University, and to prevent the loss of information that is critical to the operation of the University.

II. REFERENCES

PPM 1-12, University Institutional Data Management,
http://www.admin.utah.edu/ppmanual/1/1-12.html

PPM 1-15, Information Resources Policy
http://www.admin.utah.edu/ppmanual/1/1-15.html

PPM 1-16, World Wide Web Resources Policy
http://www.admin.utah.edu/ppmanual/1/1-16.html

PPM 2-9, Disciplinary Actions and Dismissal of Staff Employees
http://www.admin.utah.edu/ppmanual/2/2-9.html

PPM 8-10, Code of Student Rights and Responsibilities
http://www.admin.utah.edu/ppmanual/8/8-10.html

PPM 8-12-5 & -6, Code of Faculty Rights and Responsibilities
http://www.admin.utah.edu/ppmanual/8/8-12-5.html
http://www.admin.utah.edu/ppmanual/8/8-12-6.html

III. DEFINITIONS

A. Information Technology Resource (IT Resource): A resource used for electronic storage, processing or transmitting of data, as well as the data itself. Resources as defined in PPM 1-15, IV.A.

B Server: A computer used to provide information and/or services to multiple Users.

C. Security: Measures taken to reduce the risk of 1) unauthorized access to IT Resources, via either logical, physical, managerial, or social engineering means; and 2) damage to or loss of IT Resources through any type of disaster, including cases where a violation of security or a disaster occurs despite preventive measures.

D. IT Resource Steward: The individual who has policy level responsibility for determining what IT Resources will be stored, who will have access, what security and privacy risk is acceptable, and what measures will be taken to prevent the loss of Information Resources.

E. IT Resource Custodian: The organization or individual who implements the policy defined by the IT Resource Steward and has responsibility for IT systems that store, process or transmit IT Resources.

F. IT Systems Administrator: University staff that, under the direction of the IT Resource Custodian, have day-to-day operational responsibility for data capture, maintenance and dissemination.

G. User: Any person, including faculty members, staff members, students, and patients, who accesses and uses University of Utah IT Resources.

H. Private Sensitive Information: Private information retained by or accessible through IT Resources such as networks and/or computers, including any information that identifies or describes an individual, including but not limited to, his or her name, social security number, medical history, and financial matters. Access to such data is governed by state and federal laws, both in terms of protection of the data, and requirements for disclosing the data to the individual to whom it pertains.

Private Sensitive Information does not include "public information" as defined by the Utah Government Records Access and Management Act (GRAMA), or in the case of student records, "directory information" as defined by the Family Education Rights and Privacy Act (FERPA).

I. Critical IT Resource: An IT Resource which is required for the continuing operation of the University and/or its colleges and departments, including any IT Resource which, if it fails to function correctly and/or on schedule, could result in a major failure of mission-critical business functions, a significant loss of funds, or a significant liability or other legal exposure. For example, General Ledger monthly financial reporting may be considered non-Critical IT Resources by the University, but financial reporting at fiscal year-end may be considered Critical IT Resources.

J. Disaster: Any event or occurrence that prevents the normal operation of a Critical Information Technology Resource(s).

K. Disaster Recovery Plan: A written plan including provisions for implementing and running Critical Information Technology Resources at an alternate site or provisions for equivalent alternate processing (possibly manual) in the event of a disaster.

L. Unauthorized Access to IT Resources. Access to Private Sensitive Information or Critical IT Resources by a User(s) that does not need access to perform his/her job duties.

M. ISO: Institutional Security Office is responsible for the development and maintenance of security strategy for the University of Utah's computer systems and resolution of campus IT security incidents.

IV. SCOPE

A. This policy is applicable to all University of Utah colleges, departments and divisions, members of the University community, and all faculty, staff, and students. Contractors, consultants and organizations or individuals that are loosely affiliated with the University are also required to comply with this policy.

B. Specific college and/or departmental policies may be more restrictive depending on the security requirements of the college and/or department.

V. POLICY

A. University, College and Departmental Information Technology Resources

1. Protecting Private Sensitive Information

a. University colleges, departments, and divisions, must take measures to protect Private Sensitive Information that is stored, processed or transmitted using IT Resources under their control. These measures should be taken as needed and reviewed at regular intervals using best practices designated by the ISO.

b. Reasonable and appropriate security procedures must be designed to prevent unauthorized individuals or organizations from accessing IT Resources which store, process, or transmit Private Sensitive Information.

c. Security procedures must be designed for IT Resources that do not store, process or transmit Private Sensitive Information if access to such IT Resources provides the possibility of a breach of security.

2. Preventing the Loss of Critical IT Resources

    a. University colleges, departments, divisions, must take measures to identify and prevent the loss of Critical IT Resources that are under their control, at regular intervals of best practice designated by ISO, and to include Critical IT Resources in a college, department or division Disaster Recovery Plan.

    b. Reasonable and appropriate security procedures must be implemented to ensure the availability of Critical IT Resources.

B. User Information Technology Resources (Faculty Members, Staff Members, Students)

1. Protecting Private Sensitive Information

    a. Users of IT Resources must not knowingly retain on personal computers, servers, or other computing devices, Private Sensitive Information, such as Social Security Numbers, financial information including credit card numbers and bank information, or protected health information, including health records and medical information, except under the following conditions:

        i. The User must require such Private Sensitive Information to perform duties that are necessary to conduct the business of the University.

        ii. The Dean, Department Chair, or Vice President must grant permission to the User.

        iii. The User must take reasonable precautions to secure Private Sensitive Information that resides on a User's personal computer or other computing device, e.g., implement password protection for documents that contain sensitive information.

    b. Permission is not required to retain student grades, letters of recommendation, RPT documents, patentable research findings, etc., that are used regularly in the performance of faculty and staff duties. If a computer containing such data is readily accessible to unauthorized individuals, the User must take reasonable precautions to secure the data.

2. Preventing the Loss of Critical IT Resources.

    A User must take reasonable precautions to reduce the risk of loss of Critical IT Resources that reside on a User's personal computer or other computing device, i.e., backup critical documents on CDs or other media, or back up documents to a storage device or system, at regular intervals, which is administered by the User's IT Systems Administrator.

3. If uncertain whether or not an IT Resource contains Private Sensitive Information or is a Critical IT Resource, a User must seek direction from the IT Resource Steward, the IT Resource Custodian, the HIPAA Privacy Office, or the University Institutional Security Office.

C. Reporting of Security Breaches

1. All suspected or actual security breaches of university, college or departmental systems must immediately be reported to the University Institutional Security Office (security@utah.edu) or to the HIPAA Privacy Office, https://secure.uuhsc.utah.edu/privacy/) if the security breach involves protected health information, i.e., health records or medical information. IT Systems Administrators should report security incidents to the IT Resource Steward and IT Resource Custodian for their respective organization. If the compromised system contains personal or financial information (e.g. credit card information, social security, etc.), the organization must report the event to the University's Office of General Counsel. If the compromised system contains health information the organization must report the event to the HIPAA Privacy Office.

2. If Private Sensitive Information has been accessed or compromised by unauthorized persons or organizations:

a. The IT Resource Steward or User who is responsible for the information must consult with the vice president, dean, department head, supervisor, ISO and the Office of General Counsel to assess the level of threat and/or liability posed to the University and to those whose Private Sensitive Information was accessed.

b. Individuals who's Private Sensitive Information was accessed or compromised will be notified and referred to ISO for instructions regarding measures to be taken to protect themselves from identity theft.

D. Reporting Loss of Critical IT Resource

If Critical Information Resources are lost, the Data Steward or User must notify those individuals and organizations that are affected by the loss of the resource.

VI. ROLES AND RESPONSIBILITIES

A. University Institutional Security Office (ISO)

ISO reports directly to the office of the Associate Academic Vice President for Information Technology. The Information Technology Council is responsible for approving University security policies and plans. The ISO is responsible for the coordination, review and approval of procedures used to provide the requisite security for Private Sensitive Information or Critical Information Technology Resources. ISO is responsible for coordinating compliance with this policy. Responsibilities and roles include but are not limited to:

1. Develop and maintain security policy, plans, procedures, strategies, architectures, best practices, and minimum requirements in cooperation with the Information Technology Advisory Committee (ITAC), Information Technology Council (ITC), and other campus IT organizations.

2. Educate IT Systems Administrators, computer professionals, and Users, regarding security. Provide guidelines consistent with University policies, consultation, and assistance to colleges, departments and individuals regarding the proper use of computer workstations, servers, applications, department networks and other information technology resources.

3. Provide assistance in complying with this policy to IT Resource Stewards, IT Resource Custodians, and IT Administrators as requested.

4. Implement and enforce baseline perimeter security practices endorsed for educational institutions by federal, state, and local government agencies, and national organizations such as Educause and SANS.

5. Monitor and analyze campus network traffic information to ensure compliance with University security and acceptable use policies, and to evaluate, identify, and resolve security vulnerabilities, breaches and threats to University IT Resources.

6. Conduct security audits as requested by colleges or departments. Conduct security audits periodically to confirm compliance with this policy.

7. Direct the campus Incident Response Team, incident response activities, and incident resolution at the University, departmental and individual levels. Take appropriate and reasonable remedial action to resolve security incidents.

8. Assist University or third party auditors in the analysis of college and departmental IT Resources to further ensure policy compliance.

9. Monitor compliance with security policies and report compliance violations to the relevant cognizant authority.

B. NetCom Department

The NetCom department is charged with the responsibility of managing and maintaining the campus backbone network. Netcom's security roles and responsibilities include but are not limited to:

1. Monitor the campus network traffic flows, primarily for the purpose of network maintenance and optimization.

2. Inform the Institutional Security Office of traffic patterns, which pursuant to best practices, procedures and standards, may indicate a potential or actual threat to the network backbone and University IT Resources.

3. Apply security policy and procedures to campus network devices as directed by ISO, and ITAC.

C. Incident Response Team

Under the direction of the Institutional Security Office, the Incident Response Team is responsible for immediate response to any breach of security. The Incident Response Team is also responsible for determining and disseminating remedies and preventative measures that develop as a result of responding to and resolving security breaches. The team consists of the Institutional Security Office, the HIPAA Privacy Office, and designated campus IT managers.

D. IT Resource Steward

The IT Resource Steward is designated by the cognizant authority of the relevant organization. Responsibilities and roles include but are not limited to:

1. Determine the purpose and function of the IT Resource.

2. Determine the level of security required based on the sensitivity of the IT Resource.

3. Determine the level of criticality of an IT Resource.

4. Determine accessibility rights to IT Resources.

5. Determine the appropriate method for providing business continuity for Critical IT Resources (e.g., performing Disaster Recovery at an alternate site, performing equivalent manual procedures, etc.).

6. Specify adequate data retention, in accordance with University policies, and state and federal laws for IT Resources consisting of applications or data.

7. In rare cases, an organization may need to configure IT Resources in a manner that is not compatible with standard security procedures, best practices and minimum requirements (i.e., to conduct network and/or systems research, or for other academic purposes). In such cases, the IT Resource Steward, must accept responsibility for alternative security measures that may be implemented. The IT Resource Steward may request, and ISO may grant, a written exemption from standard security procedures, best practices and minimum requirements, provided the IT Resource Steward documents the need for an exception, receives an ISO assessment of the risk and vulnerabilities exposed by the exception, and agrees to make every reasonable effort to prevent the exception from causing potential or actual security threats to the relevant organization and other campus organizations.

8. An IT Resource Steward in a college or department, which lacks the professional IT staff or expertise to accomplish items (1) through (7) in this section, or to fulfill the responsibilities of the IT Resource Custodian or IT Systems Administrator, may request assistance from the University Institutional Security Office.

.

E. IT Resource Custodian

The IT Resource Custodian is responsible for implementing and maintaining security measures in accordance with the security level identified by the IT Resource Steward. For example, the Administrative Computing Services department would be the Custodian of a central student registration system. Responsibilities and roles include but are not limited to:

1. Prepare for Disaster Recovery. In the event of a disaster, provide oversight of the performance of Disaster Recovery Plans and Procedures.

2. Monitor and analyze network traffic and system log information for the purpose of evaluating, identifying and resolving security breaches and/or threats to the IT Resources of the organization for which they have responsibility.

3. Ensure that data retention requirements are met for IT Resources consisting of applications or data.

F. IT Systems Administrator

The IT Systems Administrator(s) is responsible for the performance of security functions and procedures as directed by the IT Resource Custodian and/or IT Resource Steward. It is the IT Systems Administrator's responsibility to implement and administer the security of IT Resources in accordance with University of Utah and industry best practices and standards.

VII. SANCTIONS AND REMEDIES

A. ISO may discontinue service to any User who violates this policy or other IT policies when continuation of such service threatens the security (including integrity, privacy and availability) of University IT Resources. ISO may discontinue service to any network segment or networked device if the continued operation of such segments or devices threatens the security of University IT Resources. ISO will notify the IT Resource Steward and/or Custodian or their designee to assist in the resolution of non-compliance issues before service(s) are discontinued, unless non-compliance is causing a direct and imminent threat to University IT Resources.

B. The IT Resource Steward may discontinue service or request that ISO discontinue service to network segments, network devices, or Users under their jurisdiction, which are not in compliance with this policy. IT Resource Stewards will notify or request that ISO notify affected individuals to assist in the resolution of non-compliance issues before service(s) are discontinued, unless non-compliance is causing a direct and imminent threat to University, college, or department IT Resources.

C. A User's access shall be restored as soon as the direct and imminent security threat has been remedied.

D. The University reserves the right to revoke access to any Information Technology Resource for any User who violates this policy, or for any other business reasons in conformance with applicable University policies.

E. Violation of the policy may result in disciplinary action in accordance with University policies referenced in Section II of this policy.

VIII. APPEAL PROCESS

A. Faculty may appeal violation of this policy through their cognizant authority in consultation with the ISO and the Office of Legal Counsel to informally resolve the problem. If the issue can't be resolved informally the decision may be appealed to the Office of the Senior Vice President for Academic Affairs or the Vice President for Health Sciences, depending on the department of which the faculty is a member. (See PPM XII,XI Procedures)

B. Staff may appeal to their immediate supervisor, according to policy PPM2-9 and then if needed to the supervisor at the next level higher.

C. Students may appeal through the Office of the Dean of Students as outlined in policy PPM-8-10 referenced in Section II of this policy.